Theoretical Computer Science 98 (1992) 41–50
Elsevier

Rational series with coefficients in a commutative ring

Stefano Varricchio

Dipartimento di Matematica Pura e Applicata, Università dell'Aquila, Via Vetoio, 67100 L'Aquila, Italy and L.I.T.P, Institute Blaise Pascal, Université Paris VI, Paris, France

Abstract

Varricchio, S., Rational series with coefficients in a commutative ring, Theoretical Computer Science 98 (1992) 41–50.

We extend some results of the theory of rational series with coefficients in a field to the case in which the coefficients are taken in a commutative ring. In particular, we generalize the well-known Eilenberg Equality Theorem and a recent result of Restivo and Reutenauer about the languages which are supports of rational series.

Résumé

Varricchio, S., Rational series with coefficients in a commutative ring, Theoretical Computer Science 98 (1992) 41–50.

Nous donnons quelques généralisations de résultats de la théorie des séries rationnelles à coefficients dans un corps au cas où les coefficients sont considérés dans un anneau commutatif. En particulier nous généralisons le Théorème d'Equivalence d'Eilenberg et un résultat récent de Restivo et Reutenauer sur les languages qui sont supports de séries rationnelles.

1. Introduction and preliminaries

The classical Eilenberg Equality Theorem [2] gives us an algorithm to decide the equivalence of two rational series with coefficients in a field. It states that two rational series are equal if and only if they coincide on all the words whose length is less than or equal to the sum of the dimension of two linear representations of such series. This theorem is also true when one considers series with coefficients in a division ring, or in any ring which is embeddable in a division ring. In this paper we will prove a similar result, which allows us to decide the equivalence of rational series with coefficients in any commutative ring.

In the second part of the paper we generalize a result of Restivo and Reutenauer [4]. We prove that a language L is rational if and only if L and its complementary are

supports of rational series with coefficients in a commutative ring. The proof of this result is based on some pumping properties of the supports of rational series with coefficients in a commutative ring.

The reader is referred to [1, 6] for the basic notions concerning the theory of formal power series in noncommuting variables; here we recall some notations and definitions. Let K be a semiring and A^* the free monoid on a finite alphabet A; we consider the K-module $K[[A^*]]$ of all the applications $\alpha: A^* \to K$. An element $\alpha \in K[[A^*]]$ will also be denoted by $\sum_{m \in A^*} \alpha(m)m$ or by $\sum_{m \in A^*}(\alpha, m)m$, where (α, m) denotes $\alpha(m)$. $K[[A^*]]$ is called the K-module of the *formal power series* over A^* with coefficients in K. $K[[A^*]]$ has a structure of K-algebra, where the product of two series $S, T \in K[[A^*]]$ is defined by

$$ST = \sum_{m \in A^*} \left(\sum_{uv = m} (S, u)(T, v) \right) m.$$

Moreover, if S is a series such that $(S, \Lambda) = 0$, one can define the series S^* by

$$S^* = \sum_{m \in A^*} \left(\sum_{u_1 \ldots u_k = m} (S, u_1) \ldots (S, u_k) \right) m.$$

We denote by $K[A^*]$ the subalgebra of $K[[A^*]]$ which consists of all *polynomials* over A^* with coefficients in K, i.e. those series with finitely many nonzero coefficients.

A formal power series $S \in K[[A^*]]$ is called *recognizable* if there exist a positive integer n, $\lambda, \gamma \in K^n$ and a monoid morphism $\mu: A^* \to K^{n \times n}$ such that for any $m \in A^*$ one has

$$(S, m) = \lambda \mu(m) \gamma,$$

where λ, γ are to be considered, respectively, as a row-vector and a column-vector; moreover, the triple (λ, μ, γ) is called a *linear representation* of order n.

The set of recognizable series will be denoted by $\mathrm{Rec}(K[[A^*]])$. The set of *rational series* $\mathrm{Rat}(K[[A^*]])$ is defined as the smallest subalgebra of $K[[A^*]]$ containing $K[A^*]$ and closed with respect to the star operation. In the sequel we will adopt the following equivalent notations: $K\langle\langle A \rangle\rangle = K[[A^*]]$, $K\langle A \rangle = K[A^*]$. An important theorem due to Schutzenberger states that $\mathrm{Rec}(K\langle\langle A \rangle\rangle) = \mathrm{Rat}(K\langle\langle A \rangle\rangle)$.

In this paper we will consider only rational series with coefficients in a commutative ring K. Moreover, we may always assume that K is finitely generated and unitary. Indeed, it is easy to see that any recognizable series $S \in \mathrm{Rec}(K\langle\langle A \rangle\rangle)$ has coefficients in the subring of K generated by the elements which appear in a linear representation of S and that any commutative ring is embeddable in an unitary commutative ring.

2. The equivalence problem

In this section we will give an extension of the Eilenberg Equality Theorem. Firstly, we need some decidability results in polynomial ring. Let $\mathbb{Z}$ be the ring of the positive

integers and $\mathbb{Z}[x_1, x_2, \ldots, x_k]$ the ring of polynomial in k commutative variables with coefficients in $\mathbb{Z}$. We denote by $(\mathbb{Z}[x_1, x_2, \ldots, x_k])^n$ the cartesian product of $\mathbb{Z}[x_1, x_2, \ldots, x_k]$ n times. The set $(\mathbb{Z}[x_1, x_2, \ldots, x_k])^n$ has a natural structure of module over $\mathbb{Z}[x_1, x_2, \ldots, x_k]$. The set of matrices $(\mathbb{Z}[x_1, x_2, \ldots, x_k])^{n \times n}$ is a $\mathbb{Z}[x_1, x_2, \ldots, x_k]$-algebra and it is isomorphic to $(\mathbb{Z}[x_1, x_2, \ldots, x_k])^{n^2}$ as $\mathbb{Z}[x_1, x_2, \ldots, x_k]$-module. The following theorem is a well-known result of commutative algebra.

Theorem 2.1. *The ring $\mathbb{Z}[x_1, x_2, \ldots, x_k]$ is noetherian, i.e. any ideal I of $\mathbb{Z}[x_1, x_2, \ldots, x_k]$ is finitely generated. The module $(\mathbb{Z}[x_1, x_2, \ldots, x_k])^n$ is noetherian, i.e. any submodule M of $(\mathbb{Z}[x_1, x_2, \ldots, x_k])^n$ is finitely generated.*

We recall now the following important result of computer algebra (cf. [5]).

Theorem 2.2. *Let L, M be two submodules of $(\mathbb{Z}[x_1, x_2, \ldots, x_k])^n$ given by means of a finite set of generators. It is decidable whether $L = M$.*

Let $K = \langle m_1, m_2, \ldots, m_k \rangle$ be a finitely generated commutative unitary ring. Then there is a natural epimorphism $\varphi : \mathbb{Z}[x_1, x_2, \ldots, x_k] \to K$ defined by $\varphi(x_i) = m_i$, for $1 \leqslant i \leqslant k$, and $\varphi(n) = n \cdot 1$ for $n \in \mathbb{Z}$. In this way we can identify K with $\mathbb{Z}[x_1, x_2, \ldots, x_k]/\ker \varphi$. For any nonnegative integer N we denote by $A^{[N]}$ the set of words of A^* whose length is less than or equal to N.

Lemma 2.3. *Let K be a commutative ring, $S \in \mathrm{Rec}(K \langle\langle A \rangle\rangle)$ and (λ, μ, γ) a linear representation of S of order n. Then one can effectively compute an integer N depending on S, with the property that for any $u \in A^{[N+1]}$, there exists a set $T = \{a_v\}_{v \in A^{[N]}}$, $a_v \in K$, such that*

$$\mu(u) = \sum_{v \in A^{[N]}} a_v \mu(v).$$

Proof. Let $S \in \mathrm{Rec}(K \langle\langle A \rangle\rangle)$. There exist a positive integer n, $\lambda, \gamma \in K^n$ and a monoid morphism $\mu : A^* \to K^{n \times n}$ such that for any $u \in A^*$ one has

$$(S, u) = \lambda \mu(u) \gamma.$$

We may assume that K is an unitary commutative ring generated by the set $\{\lambda_i \mid 1 \leqslant i \leqslant n\} \cup \{\gamma_i \mid 1 \leqslant i \leqslant n\} \cup \{\mu_{ij}(a) \mid 1 \leqslant i, j \leqslant n\}$. With this set we can associate a set of commutative variables $X = \{x_i \mid 1 \leqslant i \leqslant n\} \cup \{z_i \mid 1 \leqslant i \leqslant n\} \cup \{y_{ija} \mid 1 \leqslant i, j \leqslant n, a \in A\}$ and an epimorphism $\varphi : \mathbb{Z}[X] \to K$ defined by $\varphi(x_i) = \lambda_i$, $\varphi(z_i) = \mu_i$, $\varphi(y_{ija}) = \mu_{ij}(a)$, for $1 \leqslant i, j \leqslant n$, $a \in A$ and $\varphi(m) = m \cdot 1$ for $m \in \mathbb{Z}$.

Let us consider the morphism $\mu' : A^* \to (\mathbb{Z}[X])^{n \times n}$, defined by

$$(\mu'(a))_{ij} = y_{ija}, \text{ with } 1 \leqslant i, j \leqslant n \text{ and } a \in A.$$

Let $\psi : (\mathbb{Z}[X])^{n \times n} \to K^{n \times n}$ be the application defined by

$$(\psi(f))_{ij} = \varphi(f_{ij}), \text{ with } f \in (\mathbb{Z}[X])^{n \times n} \text{ and } 1 \leqslant i, j \leqslant n.$$

The map ψ is a morphism and for any $u \in A^*$ one has

$$\mu(u) = \psi(\mu'(u)). \tag{2.1}$$

For any $m > 0$ we denote by T_m the submodule of $(\mathbb{Z}[X])^{n \times n}$ generated by the set $S_m = \{\mu'(v) \mid v \in A^{[m]}\}$. In this way we construct an ascending chain of submodules of $\mathbb{Z}([X])^{n \times n}$

$$T_1 \subseteq T_2 \subseteq \cdots T_m \subseteq \cdots.$$

Since $(\mathbb{Z}[X])^{n \times n}$ is noetherian, there exists at least an integer N such that

$$T_N = T_{N+1}.$$

Such an integer may be effectively computed. Indeed for any $m > 0$, by Theorem 2.2, we have an algorithm to decide whether $T_m = T_{m+1}$ and, starting from $m = 1$, we can iterate this algorithm until we find an integer N such that $T_N = T_{N+1}$. We remark that for such an integer N it is not possible to assert that the chain terminates in T_N.

Since $T_N = T_{N+1}$, one has that for any $u \in A^{[N+1]}$, there exists a set $S = \{f_v\}_{v \in A^{[N]}}, f_v \in \mathbb{Z}[X]$, such that

$$\mu'(u) = \sum_{v \in A^{[N]}} f_v \mu'(v).$$

Therefore, by (2.1)

$$\mu(u) = \psi(\mu'(u)) = \sum_{v \in A^{[N]}} \psi(f_v \mu'(v)) = \sum_{v \in A^{[N]}} \varphi(f_v)\psi(\mu'(v))$$

$$= \sum_{v \in A^{[N]}} a_v \mu(v),$$

where $a_v = \psi(f_v)$. □

Lemma 2.4. *Let K be a commutative ring and $S \in \mathrm{Rec}(K \langle\langle A \rangle\rangle)$. Then one can effectively compute an integer N depending on S such that $(S, u) = 0$ for any $u \in A^{[N]}$ if and only if $(S, u) = 0$ for any $u \in A^*$.*

Proof. Let N be the integer of Lemma 2.3 and suppose that for any $u \in A^{[N]}$ $(S, u) = 0$. We have to prove that $(S, u) = 0$ for any $u \in A^*$. If by contradiction there exists a word w such that $(S, w) \neq 0$, we may suppose that it has minimal length and, moreover, $|w| \geqslant N + 1$. Then one can write $w = uz$ with $u \in A^{[N+1]}, z \in A^*$. By Lemma 2.3 there exists a set $T = \{a_v\}_{v \in A^{[N]}}$, $a_v \in K$, such that

$$\mu(u) = \sum_{u \in A^{[N]}} a_v \mu(v).$$

Therefore, we have

$$(S,w)=\lambda\mu(w)\gamma=\lambda\mu(u)\mu(z)\gamma=\lambda\sum_{v\in A^{[N]}}a_v\mu(v)\mu(z)\gamma$$

$$=\sum_{v\in A^{[N]}}a_v(\lambda\mu(v)\mu(z)\gamma)=\sum_{v\in A^{[N]}}a_v(\lambda\mu(vz)\gamma)$$

$$=\sum_{v\in A^{[N]}}a_v(S,vz).$$

Moreover, for any $v\in A^{[N]}$ one has $|vz|<|w|$ and $(S,vz)=0$ by the minimality of w. Thus, $(S,w)=0$, which is a contradiction. □

Theorem 2.5. *Let K be a commutative (computable) ring. There exists an algorithm to decide for any $S,T\in\mathrm{Rec}(K\langle\langle A\rangle\rangle)$ whether $S=T$.*

Proof. Let $S,T\in\mathrm{Rec}(K\langle\langle A\rangle\rangle)$. The formal series $Q=S-T$ is also regular and a linear representation of Q may be constructed from those of S and T (cf. [2]). By Lemma 2.4 we can find an integer N such that Q is identically equal to 0 if and only if $(Q,u)=0$ for any $u\in A^{[N]}$. Since K is computable, we may test whether Q is identically null and this happens if and only if $S=T$. Thus, we can decide whether $S=T$. □

3. On the supports

In this section we will consider some properties of the supports of rational series with coefficients in a commutative ring. In particular, we will prove a "pumping lemma" for these languages and subsequently we will generalize a theorem of Restivo and Reutenauer.

Lemma 3.1. *Let K be a commutative ring, $S\in\mathrm{Rec}(K\langle\langle A\rangle\rangle)$ and $L=\mathrm{supp}(S)$. Then for any infinite sequence of words $\{u_n\}_{n\geq 1}$ there exists an integer $N>0$ such that for any $n\geq N$ and for any $x,y\in A^*$ there exists an integer $i\in\{1,\ldots,N\}$, depending on n, x, and y, such that*

$$xu_1\ldots u_ny\in L \Rightarrow xu_1\ldots u_iy\in L.$$

Proof. As before, we may suppose that K is finitely generated. Let $S\in\mathrm{Rec}(K\langle\langle A\rangle\rangle)$. There exist a positive integer n, $\lambda,\gamma\in K^n$ and a monoid morphism $\mu:A^*\to K^{n\times n}$ such that for any $u\in A^*$ one has

$$(S,u)=\lambda\mu(u)\gamma.$$

Let $\{u_n\}_{n\geq 1}$ be an infinite sequence of words of A^*. For any $m>0$ we denote by T_m the

submodule of $K^{n\times n}$ generated by the set $S_m=\{\mu(u_1), \mu(u_1u_2), \ldots, \mu(u_1u_2\ldots u_m)\}$. In this way we construct an ascending chain of submodules of $K^{n\times n}$

$$T_1\subseteq T_2\subseteq\cdots T_m\subseteq\cdots.$$

Since $K^{n\times n}$ is noetherian, there exists an integer N such that

$$T_n=T_N \quad \text{for any } n\geqslant N.$$

Thus, for any $n\geqslant N$ there exist $a_1, a_2, \ldots, a_N\in K$, such that

$$\mu(u_1\ldots u_n)=\sum_{i=1,\ldots,N} a_i\mu(u_1\ldots u_i).$$

Then for any $x, y\in A^*$ one has

$$\begin{aligned}(S, xu_1\ldots u_ny)&=\lambda\mu(xu_1\ldots u_ny)\gamma=\lambda\mu(x)\mu(u_1\ldots u_n)\mu(y)\gamma\\ &=\lambda\mu(x)\sum_{i=1,\ldots,N} a_i\mu(u_1\ldots u_i)\mu(y)\gamma\\ &=\sum_{i=1,\ldots,N} a_i(\lambda\mu(x)\mu(u_1\ldots u_i)\mu(y))\\ &=\sum_{i=1,\ldots,N} a_i(\lambda\mu(x)\mu(u_1\ldots u_i)\mu(y))\\ &=\sum_{i=1,\ldots,N} a_i(S, xu_1\ldots u_iy).\end{aligned}$$

From the previous relation one derives that

$xu_1\ldots u_ny\in L \Rightarrow (S, xu_1\ldots u_ny)\neq 0 \Rightarrow \exists i\in\{1,\ldots,N\}$ such that $(S, xu_1\ldots u_iy)\neq 0 \Rightarrow \exists i\in\{1,\ldots,N\}$ such that $xu_1\ldots u_iy\in L$. □

Now in order to prove our main result, we need to introduce some preliminary notations and definitions. Let us denote by $(A^*)^\omega$ the set of all the infinite sequences $\{u_n\}_{n\geqslant 1}$ of words of A^*. Let $M:(A^*)^\omega\to\mathbb{N}$ be a map and $L\subseteq A^*$ a language. We say that L verifies the property P_M if for any $\{u_n\}_{n\geqslant 1}\in(A^*)^\omega$, $n\geqslant M(\{u_n\}_{n\geqslant 1})$ and $x, y\in A^*$ there exists an integer $i\in\{1,\ldots,M(\{u_n\}_{n\geqslant 1})\}$, depending on n, x, and y, such that

$$xu_1\ldots u_ny\in L \Rightarrow xu_1\ldots u_iy\in L.$$

We say that L verifies Q_M if both L and $A^*\setminus L$ verify P_M.

Corollary 3.2. *Let $L\subseteq A^*$ be a language such that both L and $A^*\setminus L$ are supports of rational series with coefficients in a commutative ring. Then there exists a map $M:(A^*)^\omega\to\mathbb{N}$ such that L verifies Q_M.*

Proof. By Lemma 3.1 there exist $M_1, M_2 : (A^*)^\omega \to \mathbb{N}$ such that L and $A^* \setminus L$ verify, respectively, P_{M_1} and P_{M_2}. Then, if we pose $M = \max(M_1, M_2)$, one has that both L and $A^* \setminus L$ verify P_M; thus, L verifies Q_M. □

Lemma 3.3. *Let P be a property defining a family of languages of A^*. If the following two conditions are verified,*

(a) *L verifies $P \Rightarrow \sigma^{-1}L$ verifies P for any $\sigma \in A^*$,*

(b) *the languages of A^* verifying P are finitely many,*

then any language verifying P is regular.

Proof. Let L be a language verifying P and N_L the Nerode congruence of L. One has that for any $x, y \in A^*$

$$x N_L y \Leftrightarrow x^{-1}L = y^{-1}L.$$

Since the languages $\sigma^{-1}L$, with $\sigma \in A^*$, are finitely many, N_L has finite index and, by the Myhill–Nerode theorem, L is regular. □

Lemma 3.4. *Let $L \subseteq A^*$ be a language verifying Q_M, then for any $\sigma \in A^*$ $\sigma^{-1}L$ verifies Q_M.*

Proof. Since L verifies Q_M, for any $\{u_n\}_{n \geq 1} \in (A^*)^\omega$, $n \geq M(\{u_n\}_{n \geq 1})$ and $x, y, \sigma \in A^*$ there exists an integer $i \in \{1, \ldots, M(\{u_n\}_{n \geq 1})\}$, depending on $n, \sigma x$, and y, such that

$$\sigma x u_1 \ldots u_n y \in L \Rightarrow \sigma x u_1 \ldots u_i y \in L;$$

therefore,

$$x u_1 \ldots u_n y \in \sigma^{-1}L \Rightarrow x u_1 \ldots u_i y \in \sigma^{-1}L$$

and $\sigma^{-1}L$ verifies Q_M. □

Lemma 3.5. *Let $M : (A^*)^\omega \to \mathbb{N}$ be a map. The languages of A^* verifying Q_M are finitely many.*

Proof. Suppose that there exists an integer $k > 0$ such that for any $L_1, L_2 \subseteq A^*$, verifying Q_M, one has

$$L_1 \cap A^{[k]} = L_2 \cap A^{[k]} \Rightarrow L_1 = L_2;$$

then the statement is trivially true.

Let us suppose, by contradiction, that there exist infinitely many languages of A^* verifying Q_M, then such an integer k does not exist. Hence, for any $k > 0$ there exists a word $w_k \in A^*$ and two languages $L_{1,k}, L_{2,k}$, verifying Q_M, such that

$$L_{1,k} \cap A^{[k]} = L_{2,k} \cap A^{[k]}$$

and

$$w_k \in L_{1,k}, \qquad w_k \notin L_{2,k}.$$

Moreover, we may suppose that w_k has minimal length, that is, for any $1 < |w_k|$ one has

$$L_{1,k} \cap A^{[1]} = L_{2,k} \cap A^{[1]} \quad \text{and} \quad |w_k| \geq k.$$

Let us consider now the language $L = \{w_1, w_2, \ldots, w_k, \ldots\}$. L being infinite, by König's Lemma (cf. [3]), there exists an infinite word $b \in A^\omega$ such that $F(b) \subseteq F(L)$. Thus for any $n > 0$, there exists an integer $k_n > 0$ such that $b(1)\ldots b(n)$ is a factor of w_{k_n}. So, if we pose $x_n = w_{k_n}$, $L'_{1,n} = L_{1,k_n}$, $L'_{2,n} = L_{2,k_n}$, there exist $\lambda_n, \mu_n \in A^*$ such that $x_n = \lambda_n b(1)\ldots b(n)\mu_n$ and

$$\lambda_n b(1)\ldots b(n)\mu_n \in L'_{1,n}, \qquad \lambda_n b(1)\ldots b(n)\mu_n \notin L'_{2,n}. \tag{3.1}$$

We prove now that the infinite word b may be factorized as

$$b = u_1 u_2 \ldots u_n \ldots,$$

$u_i \in A^+$, $i > 1$, with the property that for any $s > 0$ there exists an infinite sequence of positive integers $\{j_{s,n}\}_{n \geq 1}$ such that for any $n > 0$

$$\lambda_{j_{s,n}} u_1 \ldots u_s \mu_{j_{s,n}} \in L'_{1,j_{s,n}}, \tag{3.2}$$

and

$$\lambda_{j_{s,n}} u_1 \ldots u_s \mu_{j_{s,n}} \in L'_{2,j_{s,n}}. \tag{3.3}$$

We construct this sequence inductively. Let $N = M(\{b(n)\}_{n \geq 1})$. Since all the languages $L'_{1,n}$, $n > 0$, verify P_M, for any $n > N$ there exists an integer $i(n) \in \{1, \ldots, N\}$ such that

$$\lambda_n b(1)\ldots b(i(n))\mu_n \in L_{1,n};$$

moreover, since $|\lambda_n b(1)\ldots b(i(n))\mu_n| < |\lambda_n b(1)\ldots b(n)\mu_n|$, and $x_n = \lambda_n b(1)\ldots b(n)\mu_n$ is a word of minimal length verifying (3.1), one has also that

$$\lambda_n b(1)\ldots b(i(n))\mu_n \in L_{2,k_n}.$$

Since the set $\{1, \ldots, N\}$ is finite, there exists an integer $i \in \{1, \ldots, N\}$ such that for infinitely many integers $n > 0$ one has $i(n) = i$. Then there exists an infinite sequence of integers $\{j_{1,n}\}_{n \geq 1}$, with $j_{1,n} > N$, such that for any $n \geq 1$ one has

$$\lambda_{j_{1,n}} b(1)\ldots b(i)\mu_{j_{1,n}} \in L'_{1,j_{1,n}}, \ \lambda_{j_{1,n}} b(1)\ldots b(i)\mu_{j_{1,n}} \in L'_{2,j_{1,n}}. \tag{3.4}$$

Now if we pose $u_1 = b(1)\ldots b(i)$, the base of the induction is proved. Suppose now that we have constructed a sequence $u_1, u_2, \ldots, u_s \in A^+$ verifying our statement. Then there exists an infinite sequence of positive integers $\{j_{s,n}\}_{n \geq 1}$ such that for any $n > 0$

$$\lambda_{j_{s,n}} u_1 \ldots u_s \mu_{j_{s,n}} \in L'_{1,j_{s,n}}, \tag{3.5}$$

and

$$\lambda_{j_{s,n}} u_1 \ldots u_s \mu_{j_{s,n}} \in L'_{2,j_{s,n}}. \tag{3.6}$$

Let us consider the following sequence of words

$$v_1 = b(1)\ldots b(j_{s,1}),$$

$$v_2 = b(j_{s,1}+1)\ldots b(j_{s,2}), \quad \ldots, \quad v_n = b(j_{s,n-1}+1)\ldots b(j_{s,n}).$$

Since $v_1 v_2 \ldots v_n = b(1)\ldots b(j_{s,n})$ for any $n>0$, one has by (3.1)

$$\lambda_{j_{s,n}} v_1 \ldots v_n \mu_{j_{s,n}} \in L'_{1,j_{s,n}},\ \lambda_{j_{s,n}} v_1 \ldots v_n \mu_{j_{s,n}} \notin L'_{2,j_{s,n}}.$$

Let $N' = M(\{v_n\}_{n\geqslant 1})$ and, as before, we can state that for any $n>N'$ there exists an integer $i(n)\in\{1,\ldots,N'\}$ such that

$$\lambda_{j_{s,n}} v_1 \ldots v_{i(n)} \mu_{j_{s,n}} \in L'_{1,j_{s,n}}, \tag{3.7}$$

and, since $|\lambda_{j_{s,n}} v_1 \ldots v_{i(n)} \mu_{j_{s,n}}| \leqslant |\lambda_{j_{s,n}} v_1 \ldots v_n \mu_{j_{s,n}}|$, one has also

$$\lambda_{j_{s,n}} v_1 \ldots v_{i(n)} \mu_{j_{s,n}} \in L'_{2,j_{s,n}}. \tag{3.8}$$

As before, there exists $i\in\{1,\ldots,N'\}$ such that for infinitely many $n>N'$ $i(n)=i$. Thus, there exists a subsequence $\{j_{s+1,n}\}_{n\geqslant 1}$ of $\{j_{s,n}\}_{n\geqslant 1}$, such that for any $n\geqslant 1$ one has

$$\lambda_{j_{s+1,n}} v_1 \ldots v_i \mu_{j_{s+1,n}} \in L'_{1,j_{s,n}},\ \lambda_{j_{s+1,n}} v_1 \ldots v_i \mu_{j_{s+1,n}} \in L'_{2,j_{s,n}}.$$

By construction $j_{s,1} > |u_1 \ldots u_s|$ and $u_1 \ldots u_s$ is a proper prefix of $v_1 \ldots v_i$; thus, there exists $u_{s+1}\in A^+$ such that

$$u_1 \ldots u_s u_{s+1} = v_1 \ldots v_i;$$

hence, by (3.7) and (3.8), for any $n>0$, one has

$$\lambda_{j_{s+1,n}} u_1 \ldots u_{s+1} \mu_{j_{s+1,n}} \in L'_{1,j_{s,n}},\ \lambda_{j_{s+1,n}} u_1 \ldots u_{s+1} \mu_{j_{s+1,n}} \in L'_{2,j_{s,n}}.$$

In this way we can construct inductively an infinite sequence $\{u_n\}_{n\geqslant 1}$, with the required property. Moreover, for any $s>0$ the sequence $\{j_{s+1,n}\}_{n\geqslant 1}$ is a subsequence of $\{j_{s,n}\}_{n\geqslant 1}$ and for any $k>0$ $u_1 \ldots u_{k+1} = b(1)\ldots b(j_{k,i})$ for a suitable i. Thus, by (3.1), we have

$$\lambda_{j_{k,i}} u_1 \ldots u_{k+1} \mu_{j_{k,i}} \notin L'_{2,j_{k,i}}. \tag{3.9}$$

Let now $N = M(\{u_n\}_{n\geqslant 1})$. Since $A^* \setminus L'_{2,j_{k,i}}$ verifies P_M, if $k\geqslant N$, from (3.9) one has

$$\lambda_{j_{k,i}} u_1 \ldots u_s \mu_{j_{k,i}} \notin L'_{2,j_{k,i}}, \tag{3.10}$$

for a suitable $s\leqslant N\leqslant k$. As $\{j_{k,n}\}_{n\geqslant 1}$ is a subsequence of $\{j_{s,n}\}_{n\geqslant 1}$, by (3.3), one has

$$\lambda_{j_{k,i}} u_1 \ldots u_s \mu_{j_{k,i}} \in L'_{2,j_{k,i}},$$

which is in contradiction with (3.10). □

Theorem 3.6. *Let $L\subseteq A^*$. Then L is regular if and only if L and its complementary are supports of a rational series with coefficients in a commutative ring.*

Proof. If L and $A^*\setminus L$ are supports of rational series with coefficients in a commutative ring, then by Corollary 3.2 there exists $M:(A^*)^\omega \to \mathbb{N}$ such that L verifies Q_M. From Lemma 3.3, Propositions 3.4 and 3.5 it follows that L is regular. □

References

[1] J. Berstel and C. Reutenauer, *Rational Series and Their Languages* (Springer, Berlin, 1988).
[2] S. Eilenberg, *Automata, Languages and Machines, Vol. A* (Academic Press, New York, 1974).
[3] M. Lothaire, *Combinatorics on Words* (Addison-Wesley, Reading, MA, 1983).
[4] A. Restivo and C. Reutenauer, On cancellation properties of languages which are support of rational power series, *J. Comput. System Sci.* **29** (1984) 153–159.
[5] F. Richman, Constructive aspects of noetherian rings, *Proc. Amer. Math. Soc.* **44** (1974) 436–441.
[6] A. Salomaa and M. Soittola, *Automata Theoretic Aspects of Formal Power Series* (Springer, New York, 1978).